INFORMATION SECURITY THROUGH WIRELESS TECHNOLOGY[1]

PĂUNESCU, Luminiţa
University Politehnica of Bucharest,
Faculty of Automatic Control and Computers,
pauneasca2@yahoo.com

CURCULESCU, Bogdan Ionuţ
The Bucharest Academy of Economic Studies,
Faculty of Economic Cybernetics, Statistics and Informatics

Abstract

Wireless communications offer organizations and users a lot of benefits, portability and flexibility, increased productivity and lower installation costs. Wireless technologies cover a wide range of capabilities, targeted to users and their needs. Lack of wiring allows great flexibility, increased efficiency and reduced cabling costs, but there are inherent risks. Some are similar to those of wired networks, some are exacerbated by wireless connectivity, and some are new. Loss of privacy and integrity, threat and denial of service type attacks are risks normally associated to wireless communications. Unauthorized users can gain access to the information and the systems of an institution, can corrupt data, make full use of network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use their resources to launch attacks on other networks.

Keywords: *Confidentiality, integrity, availability, authentication, access points, standards*

ACM Classification: C.2.0, C.2.1, D.4.4, K.6.5

1. Goals of Information Security

When looking at information security, one must address the three tenets of information security: (1) *confidentiality*, (2) *availability* and (3) *integrity*, which will help us understand what we are trying to protect and why and all the risks and threats that face wireless communications.

Attacks on the *confidentiality* of information relate to the theft or unauthorized viewing of data, through data interception while in transit, or simply

[1]Ph.D. Student Paper

by the theft of equipment on which the data might reside, with the goal of obtaining proprietary information, user credentials, trade secrets, financial or healthcare records, or any other type of sensitive information.

Availability allows legitimate users access to confidential information, after they have been properly authenticated. When availability is compromised, the access is denied for legitimate users because of malicious activity, such as the denial-of-service (DoS) attack.

Integrity involves the unauthorized modification of information, while in transit or while being stored electronically. To protect the integrity of information, one must employ a validation technique: a checksum, an integrity check, or a digital signature.

2. **Techniques used in C.I.A. compromising**

- *Analysis* is the viewing, recording, or eavesdropping of a signal that is not intended for the party who is performing the analysis. One of the only protections available to prevent the loss of confidentiality is *encryption*. The risk of analysis on an RF signal is an inherent risk that cannot be avoided. The only option is to mitigate the risk with some type of confidentiality control.
- *Spoofing* is the act of impersonating an authorized client, device, or user to gain access to a resource that is protected by some form of authentication or authorization. Spoofing in wireless networks, it primarily involves an attacker setting up a *fake access point* to get a valid client to pass authentication information to that attacker. Another way attackers spoof is by performing a *man-in-the-middle* attack, when an attacker would position himself between a client and the network. This could be accomplished by spoofing a valid access point or by hijacking a session. Once this part is complete, the attacker would then use the authentication information provided by the client and forward it to the network, subsequently using its resources.
- Using the *Denial-of-service (DoS)* attack, a network device or entire network will be unable to communicate. Wireless DoS attacks can be achieved with small signal jammers.
- *Malicious code* can infect and corrupt network devices; it comes in many forms: viruses, worms, and Trojan horses.
- *Rogue access points* pose a major threat to any organization, because of the high availability and the limited security features. If a company does not approach the WLAN (wireless local area network) concept fast enough, frustrated employees will take it upon themselves to start the process, putting in wireless systems of their own. This has created a real threat because now a user can easily bring in a rogue access point, plug it in, and put the entire network at risk. The knowledge level required to install an off-the-shelf access point is minimum, plug-and-play device is the only step needed. These same people lack the ability to secure these devices or even understand the risk they are posing for the company.

As an immediate countermeasure, many companies that jumped into the newly formed wireless security market, have adapted and created tools to detect rogue access points. Some companies have used rogue access points scenarios, by creating policies about wireless usage and strict penalties for rogue access placement. The last alternative was the investment in wireless intrusion detection systems (WIDS).

The Radio Frequency Identification (RFID) concept has created some major privacy issues. With RFID, companies can save time and money by being able to track products from their creation, to their purchase at a retail store, and beyond. It is the beyond part that has so many people upset about the inherent privacy issues of RFID. Only recently has their true potential been realized.

Such a system is a small tag that is affixed to an object to allow that object to be tracked. Once this tag has been turned on or energized, it will send information about itself when a reader queries it. This tracking can take place wherever there is a reader ready to query the tag. This means other companies can read RFID tags from their suppliers. There also is the ability to add to these tags, gathering enormous data quantities.

When discussing RFID, the first thing that comes to mind is the concern over privacy. In a world where the products one consumes transfer information to anyone willing to listen, the opportunity to market and collect data about us becomes a real concern. Some people have talked about many things relating to RFID, from the wild conspiracy theories to real issues that affect everyone on an every-day basis.

What is absolutely certain is the RFID might allow a simple object to become a tracking device; a great inconvenient but technically possible.

3. **Wireless LAN security standards**

Wireless communications were always prone to security issues well before any of the 802.11 standards. Most people never thought about wireless security until the market responded with news, ads, and products to make the public aware of the dangers. What makes wireless such a security threat has to do with the fact that it is wireless. This means that data is transmitted over airspace and is susceptible to eavesdropping by anyone in a given area. Over the years, different types of encryption have been used to protect the data inside this transmission; however, this has not always been successful.

When connecting to a wireless network, one must perform some type of authentication. There are two main types of authentication per the current IEEE standards: share key authentication and open key authentication, according the IEEE standards: WEP, 802.1x, RADIUS, EAP, WPA, 802.11i, and WAPI.

3.1. *WEP*

The *Wired Equivalent Privacy (WEP)* standard was created to give wireless networks safety and security features similar to that of wired networks. WEP is defined as the optional cryptographic confidentiality mechanism used

to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.

The WEP protocol is used to encrypt data from a wireless client to an access point. This means the data will travel unencrypted inside the wired network. The WEP protocol is based on RSA Securities'RC4 stream cipher. This cipher is applied to the body of each frame and the CRC.

There are two levels of WEP commonly available: (1) one based on a 40-bit encryption key and 24-bit initialization vector, which equals 64 bits; and (2) one based on a 104-bit encryption key and 24-bit initialization vector, which equals 128 bits. This protocol has been plagued with issues since its inception. A magnitude of exploits, poor design elements, and general key management problems have made WEP a very insufficient security mechanism. One of the original functions of WEP was to have the encryption unable to be affected by loss of the frame due to interference. What this means is when one sends data across the air and loses the frame, there would be no loss to the previous frame. With newer security methods and older wired secured methods, it is common for subsequent packets to have an encryption dependency on the next or previous frame.

3.2. *802.1x*

Both the IEEE and ANSI organizations approved the 802.1x standard. The 802.1x standard was designed for port base authentication for all IEEE 802 networks. This means it will work across Ethernet, FDDI, token ring, wireless, and many other 802 networking standards.

One thing people tend to become confused about is that 802.1x is in no way any type of encryption or cipher. All the encryption takes place outside the 802.1x standard. For example, on a wireless network, the EAP would use one of its various methods of encryption for authentication. After the user authenticates to the wireless network, they may start a conversation using WEP, TKIP, AES, or one of the many other standard wireless encryption schemes. When looking at the 802.1x standard, at its most basic view one sees actually what it was intended for, port-based authentication. This means the standard takes the authentication request, decides if it is or is not allowed onto the network, and then grants, or revokes, access.

Many parts of how 802.1x works are within other standards, such as EAP and RADIUS. The 802.1x standard is just a mechanism that denies all traffic except EAP packets from accessing the network. Once the EAP says it is OK for the device to access the network, the 802.1x protocol tells the switch or access point to allow user traffic. This is accomplished by having the network port or, in a wireless situation, each client connection in one of two port states. These states are controlled and uncontrolled.

Figure 1 reveals the three main designations called out by the 802.1x standard. Each of them has specific rules and functions. The standard was written to incorporate a large amount of different equipment; the names of these functions remain somewhat generic. As one can see from the figure, the 802.1x protocol leverages two other standards. From the supplicant to the

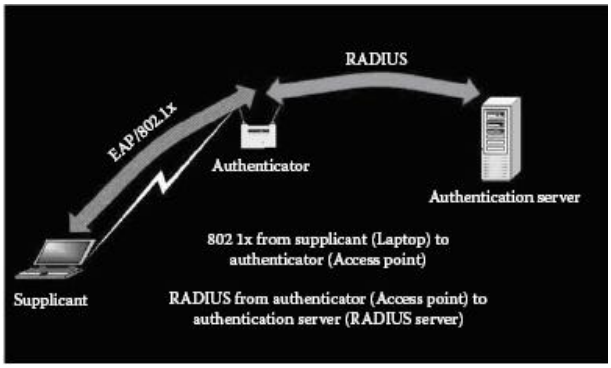

Figure 1. *802.1x overview*

authenticator, the standard is EAP. From the authenticator to the authentication server, the protocol is RADIUS. The 802.1x protocol takes EAP requests, sends them to a RADIUS server, and waits for an answer. Once this answer is received, it will allow or deny access to the network.

Looking at each of the technical parts in communication flow from fig.1, one can explore the key roles in the 802.1x standard: the authentication server, authenticator and supplicant. They each perform specific roles in processing the authentication exchange and allowing correctly authenticated devices or users onto the network.

The authentication server provides the access granting and access rejecting features. It does this by receiving an access request from the authenticator. When the authentication server hears a request, it will validate it and return a message granting or rejecting access back to the authenticator. This is the back end of the 802.1x standard and, per the standard, the operation of this server is defined in another standard (i.e., RADIUS).

The **authenticator** is the first piece of network electronics that an 802.1x device will attempt connection. In this example, it is a wireless access point, although it can be anything providing access to the network. The device's role is to let only EAP packets pass through and then wait for an answer from the authentication server. Once the authentication server responds with an accept or reject message, the authenticator acts appropriately. If the message is returned, it is a reject message and it will continue to block traffic until the result is an access accept. When the accept response comes from the authentication server, the authenticator then allows the supplicant the ability to access the network.

The **supplicant** is the device that wants to connect to the 802.1x network. This can be a computer, laptop, PDA, or any other device with a network interface card. When the supplicant connects to the network, it must go through the authenticator. This authenticator only allows the supplicant to pass EAP request traffic destined for the authentication server. This EAP traffic is the user's or device's authentication credentials. Once the authentication server determines that the user or device is allowed on the network, it will send an access-granting message.

3.3. *RADIUS*

RADIUS (*Remote Authentication Dial-In User Service*) is a protocol used in network environments for authentication, authorization, and accounting. RADIUS can run across many types of devices, such as routers, servers, switches, modems, VPN concentrators, or any other type of RADIUS-compliant device. The protocol works by creating an encrypted tunnel between the network device and the RADIUS server. This tunnel is used for sending all the *Authentication Authorization Accounting (AAA)* information about who a user is, where the user is allowed to go, and where the user actually did go. To start this encrypted tunnel, a phrase or password called the shared secret is needed. The shared secret is located on the RADIUS participating network device and the RADIUS server. Once the shared secret is correctly set up, secure communication can take place.

This protocol allows administrators to centrally locate and administer user access and accounting for all network equipment as well as remote access. RADIUS prevents many of the headaches associated with properly removing access to network equipment when employees are terminated. Once an organization has deployed RADIUS, user access could easily be removed in the event of a termination, unlike in the old days when administrators would have to manually change usernames and passwords on all network equipment.

RADIUS could be used as an access method to administer the access point, similar to how it would be used to administer routers or switches. The access point and the RADIUS server would have a shared secret and that would be used to set up an encrypted channel that can carry user authentication traffic.

3.4. *EAP*

Extensible Authentication Protocol (EAP) is a standard method of performing authentication to gain access to a network. The industry decided it was easier to make an authentication protocol act the same way no matter how or what type of authentication validation took place. This meant that for the first time a protocol could be inserted into products and software that allowed for passwords, tokens, or biometrics without having to write any extra code to support the different methods. This is how and why EAP was created. To use EAP, one must specify inside the type field what kind of authentication one is going to use. EAP can adapt to security issues and changes by leveraging different methods of authentication.

One of the main points in using EAP is the ability to leverage multiple types of authentication mechanisms. This has helped EAP from becoming obsolete due to security vulnerabilities or protocol weaknesses. The original standard only lists three main EAP types. These types are MD5 Challenge, One Time Password (OTP), and Generic Token Card (GTC). Today there are a number of different EAP types, some of which are vendor specific, some detailed in the EAP standard, and some detailed within their own standard documents.

3.5. *WPA*

Wi-Fi Protected Access (WPA) has an interesting history in relation to how it became a standard. When the security of WEP was broken, the industry turned to the IEEE to fix it. The IEEE said it would create the 802.11i wireless security standard. This standard dragged on and was very slow moving. As it took longer and longer to ratify, wireless device sales declined, due to the lack of a standard secure wireless networking method. With this all-so-needed standard lacking, the wireless manufacturers started to push the IEEE and other standard boards to ratify something so they could produce secure standard products. With the pushback of the 802.11i release date, the Wi-Fi Alliance decided that it would create a subset 802.11i standard called WPA. The Wi-Fi Alliance created WPA by leveraging what the 802.11i task group had already done and formalized it into WPA. This meant that any major changes to the 802.11i standard would influence future versions of WPA.

The WPA standard supports two methods of authentication and key management. The first one is EAP authentication with the 802.1x standard. This method works through the use of the 802.1x protocol and a back-end authentication server. It leverages EAP for in-air authentication and RADIUS for back-end authentication. This method is the more secure of the two and provides the lowest amount of end-client administration. The next available option is to use pre-shared keys. This option requires that a key be applied to the devices and wireless access points. This also means that everything has the same password entered. To combat someone using this key to eavesdrop on others conversations, WPA uses a method that creates a unique session key for each device. This is done by having a pre-shared key called the group master key (GMK) that drives a pair transient key (PTK). This second solution was added to WPA for home and small office support.

3.6. *802.11i*

The *802.11i* security standard came about in response to the need to improve the security of 802.11 networks to a level sufficient to warrant wireless as a generally accepted secure transport medium. In this standard, the IEEE outlined a secure way to access wireless networks. It also tried to mitigate the now-enormous amount of threats that were making wireless networking a real risk for companies.

Looking at 802.11i up close, one notices that it uses a number of standards, protocols, and ciphers, which have already been defined outside the 802.11i (RADIUS, 802.1x, EAP, RSN).

The Robust Security Network (RSN) standard is used for dynamic negotiation of authentication and encryption. It is used to negotiate what kind of encryption a client can support as well as what type of encryption is required based on a policy.

It was determined that the 802.11i standard would not specify an authentication method or type; rather, it would allow a protocol that can perform multiple types of authentication inside itself. This is exactly what EAP does;

it allows the use of many different authentication types from passwords, smart cards, certificates, and many others based on the same request, accept, and reject methods. For EAP to work correctly with the 802.11i standard, another well-known standard must facilitate the transmission of EAP between untrusted and trusted entities. This is where the 802.1x standard fits in; its main goal is to provide a framework for strong authentication and key management. The 802.1x protocol allows the access point only to permit an EAP request into the network. This is the case until the client is properly authenticated. Once authenticated, key negotiation and subsequently network access, can be achieved.

As included in WPA, the 802.11i standard needed an option for environments in which an authentication server was not financially feasible. This authentication server was a requirement of the 802.1x standard., to make 802.11i viable for both large enterprises and small office/home office users, another method was necessary. This is where the pre-shared key method originated. This is very similar to WPA and its pre-shared key method. When a pre-shared key is used, each client uses a secret to create subsequence-keying material. This master key is the same across the network, just like WEP, although it is used to create a session-based key for each client.

3.7. *Wi-Fi Protected Access (WPA2)*

After 802.11i came out, the Wi-Fi Alliance wanted to continue the initial investment made in WPA. This created an issue because the 802.11i standard was now out and another standard was not what the industry needed. To keep WPA going, the Alliance decided it would go back to the core benefit the organization provided - standard interoperability testing and certification. In creating WPA2, the Wi-Fi Alliance made this version of WPA an interoperability mark similar to Wi-Fi. This mark ensures that any product carrying it has an interoperable 802.11i standard.

3.8. *WLAN Authentication and Confidentiality Infrastructure (WAPI)*

China has decided that 802.11i is taking too long and they are better off creating their own standard, which has led to the creation of the *WLAN Authentication and Privacy Infrastructure (WAPI)* standard. This standard has many similarities to 802.11i, such as RADIUS and 802.1x. Getting any information about this standard is a violation of Chinese national security under China's State Council Directive 237, which regulates commercial encryption ciphers and requires encryption technology to be developed and sold under a blanket of secrecy.

4. **Authentication**

When connecting to a wireless network, based on the early mentioned standards, there are two used mechanisms, each of them with their own characteristics and vulnerabilities:

4.1. *Shared key authentication*

Shared key authentication was created to be the more secure of the two types; however, as we will shortly see this actually became the less secure due to a small oversight in how it validates user keys.

Shared key authentication works via a challenge response mechanism. To explore this process, one must first connect to the network, by having the client device send out a probe frame. This frame will look for available wireless networks and their connection settings. Once an access point hears a probe, it will respond with a probe response frame. This frame will identify all of its connection settings to the end device. In some cases, an end device will hear many responses from different access points in the area. To make sure that the end device connects only to the access point with the best signal, the probe response frame has a value for current signal strength. A client might hear multiple replies, although it will only connect to the access point with the highest signal strength value. Once the end client hears this and determines that it supports the same settings as the access point, the next portion (called authentication) takes place.

When the end device wants to authenticate, it sends an authentication response frame to the access point. This frame is evaluated; once the access point determines it is an authentication request, it will send a challenge packet back to the client, with clear-text piece of data. The end device is required to encrypt this data with its WEP key and sends it back to the access point. Once this is done and the access point receives the packet, it checks it against what it has for the encrypted version of that packet. If the results match, the access point will allow the end device onto the network. If the results do not match, the authentication fails and the end device is denied a connection (the connection and authentication process are illustrated in fig. 2).

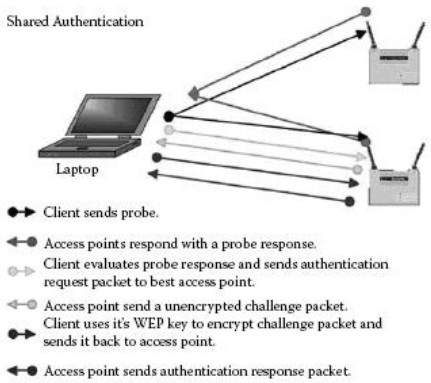

Figure 2. *Shared Key Authentication*

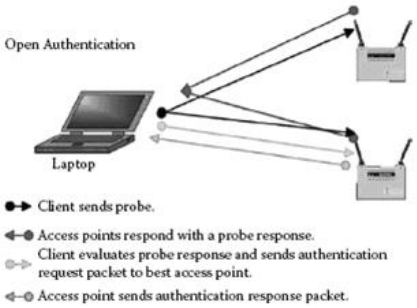

Figure 3. *Open Key Authentication*

4.2. *Open key authentication*

Open key authentication was originally seen as less secure than shared key authentication. The intent was to make an open network, thus not requiring clients to have knowledge of the WEP key. As security became an increasingly visible issue, many vendors turned to the drawing board, in order to come up with a solution that improves security, while staying within the standard guidelines. These efforts led to the idea of using open authentication and, unlike before, this open authentication would require the use of a WEP key. When used, the WEP key was required to connect to the network. This worked because when one talked with the right WEP key, one's cyclic redundancy check (CRC) passed its test and the frame was allowed to access the network to it destination.

Looking at how open authentication works (fig. 3), one sees that the end device is connected to the network as it did with shared key. It makes a probe request, listens to probe responses from multiple access points in the area, and then determines the best access point to make a connection with based on signal strength.

How do open and shared key authentications differ? Open authentication sends an authentication request but does not receive a challenge, but instead, it is allowed to talk by default. When WEP is enabled, the process is slightly different. When the wireless client starts to talk, it automatically encrypts all the data with WEP encryption. When the access point hears data being sent, it decrypts the frames and forwards them. If the frames are encrypted with a different key than the access point, the decryption portion fails and the packet is dropped.

5. **Wireless Security Architectures**

When discussing securing wireless, one needs to understand how to create different wireless security architectures. The four high-level architectures are:

1. Static WEP
2. VPN
3. Wireless firewall or gateway device
4. 802.1X

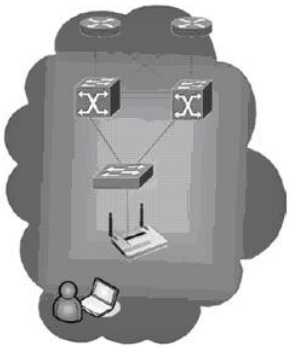

Figure 4. *Static WEP wireless architecture*

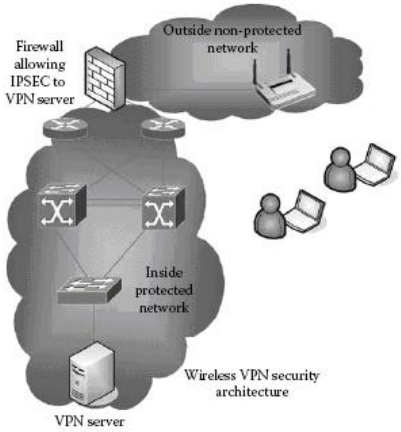

Figure 5. *Wireless VPN architecture*

5.1. *Static WEP Wireless Architecture*

The first architecture is static WEP, what the majority of wireless deployments are running today. Most companies are trying to change this into one of the other, more secure architectures. Still, WEP has some merits, such as speed and its standardization. A lot of old wireless equipment is only able to support WEP and WEP only. WEP is located inside a number of 802.11 standards, that led to wide adoption of these technologies and security standard. Figure 4 details how the network should be set up to support WEP. In this architecture, all the access points should be thought of as an extension of the wired network. Each access point is plugged into a switch similar to how a hub could extend the port count on a wired network.

Some of the major problems with WEP include security and manageability. A large number of attacks have been released against the WEP protocol. The WEP protocol also requires tremendous management efforts, which include the labor involved to distribute the static network keys to all devices that are required to connect to the network.

A solution can be created using WEP; and although it will not be the

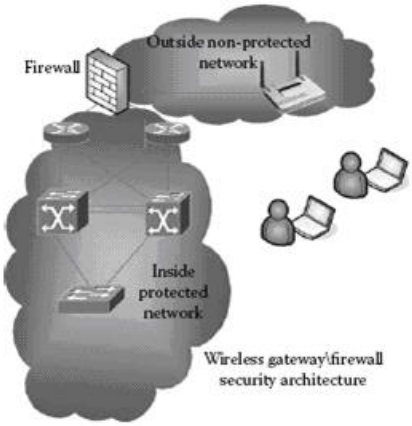

Figure 6. *Wireless Gateway*

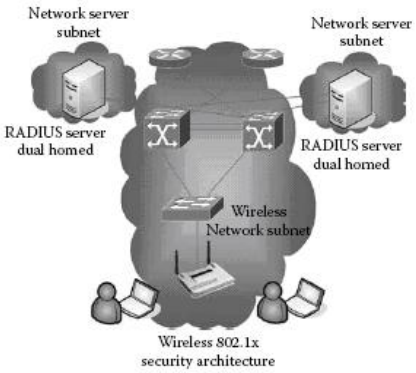

Figure 7. *Wireless 802.1x Security Architecture*

most secure solution, it is the least expensive hardware-requiring architecture. When talking about cost, WEP is one of the most inexpensive solutions because it is already in all standard 802.11/b/g/a access points. Nothing other than the access points and the client cards are required to support WEP. The support of WEP is already included in the 802.11, 802.11b, 802.11a, and 802.11g standards.

Using a WEP solution for small to mid-size companies can prove inexpensive in the short term and costly in the long term. The major cost of WEP is not in the deployment; performing a first-time setup of WEP is simple even in large companies. Tools are available to set up clients with simple executable files. These can be pushed with Microsoft group policy or manually installed by IT staff members.

The real cost of WEP lies in support and ongoing key management. The first time a key is compromised, a full re-key of everyone is needed. This means the cost associated with the security keying of the first deployment of clients will become a reoccurring cost until another security solution is deployed.

Looking at WEP from a risk perspective, it is one of the most risky wire-

less security standards out there. There are a number of tools available to crack WEP. Another downside to WEP is management, re-keying is a major effort. In a large environment, this can pose a major problem and the outcome could be a decision not to re-key. One of the other issues with WEP is that it is only a computer-based authentication mechanism. This means if someone were to steal a laptop already set up to connect to a WEP-enabled network, that machine would connect, no matter who was using it.

5.2. *VPN*

The next architecture is the virtual private network (VPN) approach. In this architecture, one takes all the wireless airspace and treats it as a public network such as the Internet. This will be done at a policy level and at a technical level, segmenting the wireless network and locating it outside the local trusted network. This would mean that all wireless access is very similar to remote access. The wireless clients will have to establish a VPN session with a wireless firewall, gateway, or VPN concentrator on the inside of the network.

VPN creates encrypted tunnels in public networks. This is done in order to connect two private networks and extending them to connect multiple private networks, in an encrypted extranet. VPNs protect confidentiality and integrity through encryption.

5.3. *Wireless Gateway Systems*

The next architecture is the wireless gateway or firewall. In this architecture (fig. 6), the wireless network is segmented from the wired network in a similar way as in the VPN architecture. This means the wireless access points and their clients are outside the corporate firewall. With this architecture, the firewall or gateway allows or denies the wireless and devices' access. This access can be set to different resources beyond it. Some of these devices have the ability to select groups based on user credentials and allow or deny the client to different portions of the internal network. For example, a group could be created only allowing the wireless end devices to access the Internet or maybe a single server sitting deep inside the internal network.

When one looks at using wireless gateways or firewalls, one must contrast the pros and cons of any architecture. Looking at the pros, one first notices that guest sign-on is supported by almost all wireless gateways or firewalls in this category. One also notices support for access control lists that are based on a number of advanced objects. These objects can be accounts, devices, or network segments. Having flexibility in a security product is always an added bonus. During the life cycle of any security appliance, user requirements are often pushing device features that should be limited to only a select few. Being able to accommodate these select few without giving everyone else the same level of access is what makes these devices shine.

Each device has different features and functions as to how they operate. Some devices can encrypt communications at the data link or MAC layer, beyond what any VPN device can do, because it needs the MAC and IP layer

to send and receive packets. A VPN device can mask the IP layer using only a gateway-to-gateway communication structure, although this is very unlikely in reference to a wireless VPN solution. When two devices are talking, all one can see is the sender's and receiver's MAC address; all other communication is encrypted.

Looking at some of the disadvantages to this architecture as a whole, one notices that these devices do nothing to protect transmission over the airwaves. All the security features of these devices take place only once the data has crossed through the product itself, if all the wireless threats can be exploited over the airwaves until they pass through the gateway device. The only slight mitigation is seen with the advent of link layer encryption.

One of the advantages of this is in the event that the wireless becomes compromised, getting into the network still requires defeating the security of an appliance.

5.4. *802.1x*

The 802.1x architecture involves another approach, different from the ones discussed previously. This architecture is the general direction of the IEEE 802.11i standard. A number of companies have taken this direction to lay the groundwork for the 802.11i standard. Currently, the 802.11i standard is out, although many products are just starting to utilize it. All the pieces that make up 802.11i are located in the 802.1x architecture. This 802.1x architecture involves keeping wireless networks safe using an EAP-encrypted channel to send authentication traffic into the network. Once validated, one is granted access to the network. Until this validation takes place, the only traffic allowed to pass into the network is the EAP authentication traffic.

Looking at the architecture detailed in fig. 7, one can see that no longer is the wireless considered hostile and in need of separation from the rest of the network. This is due to the prevention of traffic flowing through the access point into the network. With the 802.1x standard, the only traffic one can pass without authentication is authentication traffic. To support this architecture, one needs the three key pieces that make up the 802.1x standard. The supplicant is needed and is present as a wireless client. The authenticator is needed and is made up, in this case, of the access points. The third piece needed is one that is added from the other solutions, the authentication server. In this case and most other 802.1x cases, a RADIUS server is used to fulfill this piece.

Now that each of the pieces has been identified, one can see the solution in action. When a client connects to the network, the access point will ask it to provide authentication via EAP. Depending on which EAP type is used, different authentication methods inside each EAP type take place. No matter what EAP type is used, a successful authentication is signaled to the access point by an EAP success message. Once this message is relayed from the authentication server to the access point, the access point will let the supplicant or wireless client onto the network.

6. Conclusions

The risks related to wireless technology use are considered. Many of the today communication protocols and commercial products don't offer sufficient security, which represents unacceptable risks for company's regular activities.

Such risks must be actively addressed, to protect the sustaining capacity of essential operations, before we use these technologies. Even more, many organizations have a bad wireless technology management, such examples including the development of "factory flaws" equipment, which can not control or inventory the access points, can't implement the provided security capabilities and can not develop or employ appropriate security architecture for the wireless environment. In most part, the risks can be reduced, however, there must maintain a balance between technical solutions and their implementation costs. Currently, traders and community standards work aggressively to obtain more robust, open and secure solutions. For these reasons, it would be safer for some agencies to wait for some more mature solutions.

References

1. Walker, J., *Unsafe at Any Key Size: an Analysis of the WEP Encapsulation*, "Tech. Rep. 03628E", IEEE 802.11 committee, March 2007.
2. Blunk, L., and Vollbrecht, J., *PPP Extensible Authentication Protocol(EAP)*, "Tech. Rep. RFC2284", Internet Engineering Task Force (IETF), March 1998.
3. Lucent Orinoco, *User's Guide for the ORINOCO Manager's Suite*, November 2000.
4. Borisov, N., Goldberg, I., and Wagner, D., *Intercepting Mobile Communications: The Insecurity of 802.11*, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
5. Earle, E.A., *Wireless security handbook*, "Auerbach Publications", 2006.
6. Walker, J., *Overview of 802.11 security*, http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15 _TG3-Overview-of-802-11- Security.ppt, March 2001.
7. "IEEE 802.11Working Group", http://grouper.ieee.org/groups/802/11/index.html.
8. Gallegos, F., Manson, D., and Allen-Senft, Sandra, *Information Technology Control and Audit*, "Auerbach", 1999.
9. Walsh. J. (ed), *Asset Protection and Security Management Handbook*, "POA Publishing LLC", 2002.
10. Tiller, J.S., *The Ethical Hack: A Framework for Business Value Penetration Testing*, "Auerbach", 2004.